

I hereby certify that this paper is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Asst. Comm. for Patents, Washington, D.C. 20231, on this date.

12/12/00
Date

Express Mail Label No.: EL769181522US

PSEUDO-CHAOTIC COMMUNICATION METHOD
EXPLOITING SYMBOLIC DYNAMICS

This invention was made with government assistance provided by the Army Research Office (DAAG55-98-1-0269). The government has certain rights in this invention.

FIELD OF THE INVENTION

The field of the invention is data communication. The invention is particularly applicable to ultra-wide bandwidth impulse-radio communication systems.

BACKGROUND OF THE INVENTION

The continually increasing reliance on wireless forms of communication creates reliability and privacy problems. Data should be reliably transmitted from a transmitter to a receiver. In particular, the communication should be resistant to noise, interference, and possibly to interception by unintended parties.

In the last few years there has been a rapidly growing interest in ultra-wide bandwidth (UWB) impulse radio (IR) communication systems. These systems make use of ultra-short duration pulses that yield ultra-wide bandwidth signals characterized by extremely low power spectral densities. UWB-IR systems are particularly promising for short-range wireless communications as they combine reduced complexity with low power consumption, low probability of detection (LPD), immunity to multipath fading, and multi-user capabilities. Current UWB-IR communication systems employ pseudo-

1 random noise (PN) coding for channelization purposes and pulse-position modulation
2 (PPM) for encoding the binary information.

3 Others have proposed aperiodic sequences of pulses in the context of
4 chaos-based communication system. Additional work has relied upon the self-
5 synchronizing properties of two chaotic systems. In such a system, data is modulated into
6 pulse trains using variable time delays and is decodable by a coherent receiver having a
7 chaotic generator matched to the generator used in the transmitter. Such system is known
8 in the art as a Chaotic Pulse Position Modulation (CPPM) scheme.

9 Such chaotic dynamical systems have been proposed to address the
10 problem of communication privacy. Chaotic signals exhibit a broad continuous spectrum
11 and have been studied in connection with spread-spectrum applications. The irregular
12 nature of a chaotic signal makes it difficult to intercept and decode. In many instances a
13 chaotic signal will be indistinguishable from noise and interference to receivers not
14 having knowledge of the chaotic signal used for transmission. In the context of UWB
15 systems the use of nonperiodic (chaotic) codes enhances the spread-spectrum
16 characteristics of the system by removing the spectral features of the signal transmitted.
17 This results in a lower probability of interception/detection (LPI/LPD) and possibly less
18 interference towards other users. This makes the chaos-based communication systems
19 attractive.

20 There remains a need for improved chaotic coding/modulation methods to
21 produce such attractive communication systems. It is an object of the invention to meet
22 that need.

SUMMARY OF THE INVENTION

The invention is a pseudo-chaotic coding/modulation method. The coding method of the invention exploits symbolic dynamics of a chaotic map at the transmitter to encode data. This produces an encoding system that synthesizes the chaotic map based upon the data to be transmitted.

In a preferred embodiment, pseudo-chaotic iterates are generated from a digital implementation of a Bernoulli shift map. The output of the shift map is translated by a mapping, preferably implemented by a digital signal processor, to allow transitions between states in a transmitted signal to differ, and the translated map is used to drive a modulator (for example PPM, FSK, PSK, QAM, etc.). In the specific case of pulse-position modulation (PPM) the translated map is used to modulate pulse train positions within a periodic synchronization frame. The preferred embodiment uses a shift register to implement an approximation of the Bernoulli shift map acting as a form of convolutional code with a number of states equal to the symbolic states defined on the chaotic map. A receiver may use fewer states and still decode the data signal, allowing receiver scalability.

A preferred transmitter accepts digital data for coding. The digital data is allocated to symbolic states according to a chaotic map. The pseudo-chaotically coded data is converted to analog form and modulated into synchronization frames in a transmitted signal.

Another preferred embodiment accepts digital data for coding. The digital data is encoded by applying a chaotic map having N states, where $N=2^M$, with M being the number of bits in the shift register implementing the Bernoulli shift map. The symbolic states are defined on the chaotic map according to a Markov partition and the sequence of the states constitutes the encoder output. The pseudo-chaotically coded data is converted to analog form and modulated to produce a modulated signal for transmission.

1 The preferred embodiments thus include features to produce useful coding,
2 decoding, and modulation methods. Artisans will understand the important features may
3 be applied to communication systems in different ways while still realizing advantages of
4 the invention.

6 BRIEF DESCRIPTION OF THE DRAWINGS

7 Other features, objects and advantages of the invention will be apparent by
8 reference to the detailed description and the drawings, of which:

9 FIG. 1 is a block diagram of a preferred pseudo-chaotic coding/modulation
10 method of the invention;

11 FIG. 2 illustrates a Bernoulli shift map with the definition of the symbolic
12 dynamics in accordance with a preferred embodiment of the invention;

13 FIG. 3(a) illustrates implementation of the Bernoulli shift map through the
14 M-bit shift register and D/A converter of FIG. 1;

15 FIG. 3(b) illustrates the effect on state quantization by the shift register of
16 FIG. 3(a) with $M=4$;

17 FIG. 4 illustrates an effect of a Gray/binary translation from the Bernoulli
18 shift map to a tent map;

19 FIG. 5 illustrates a preferred periodic synchronization frame for the
20 modulation conducted by the transmitter of FIG. 1 when pulse-position modulation is
21 used;

22 FIG. 6 shows the tent map having the same definition of the symbolic
23 dynamics as in FIG. 2 and illustrating the symbolic states definition according to a
24 Markov partition with $N=8$ states;

25 FIG. 7 illustrates the transition state diagram associated to the dynamics of
26 the tent map with the state definition illustrated in FIG. 6; and

27 FIG. 8 illustrates the trellis diagram associated with the transition state
28 diagram of FIG. 7.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to FIG. 1, a preferred embodiment system constructed according to the invention includes a transmitter/encoder 10 that communicates with at least one receiver/decoder 12 over a channel 14, typically (but not necessarily) a wireless channel. The encoder 10 accepts a data stream and transmits data into the channel 14 using a pseudo-chaotic encoding. In the preferred embodiment, coding is conducted primarily by a shift register 16 that implements an approximation of a Bernoulli shift and a digital signal processor 18. The digital signal processor translates dynamics of the Bernoulli shift register, while permitting simple transformations, e.g. a Gray/binary conversion, or the realization of more complex pseudo-chaotic maps, which might be used for spectral shaping purposes and/or to enhance maximum likelihood detection by the receiver/decoder 12. Output from the digital signal processor is converted by a D/A converter and used to modulate data in a modulator 22. In a preferred embodiment, pulse-position modulation is used in a periodic synchronization frame. In general, the symbolic dynamics approach enables realization of a Viterbi detector 24 in the receiver with a number N_R of states lower than the levels in the transmitter.

I. Encoding

A. Shift Map

In the preferred embodiment of FIG. 1, the shift register 16 implements a shift of an incoming bit stream. In considering the preferred embodiment and the implemented shift, symbolic dynamics theory will be helpful in aiding understanding of the invention.

We first consider the shift map and resulting symbolic dynamics. Σ_2 indicates the symbol space of binary "0"s and "1"s, that is $\Sigma_2 = \{(s_0 s_1 s_2 \dots) : s_i = 0 \text{ or } s_i = 1\}$. Then, the shift map $\sigma: \Sigma_2 \rightarrow \Sigma_2$ is defined in Equation (1) as:

$$\sigma(s_0 s_1 s_2 \dots) = s_1 s_2 s_3 \dots \quad (1)$$

that is the shift map simply "forgets" the first entry in a sequence, and shifts all other entries one position to the left. Incidentally, the shift map is perhaps the simplest example of chaotic dynamics and it possesses all the peculiar features of chaotic systems.

An equivalent way of studying the shift map is to represent the state x of the corresponding discrete (one-dimensional) dynamical system as a binary expansion, as in Equation (2):

$$x = 0.b_1 b_2 b_3 \dots \equiv \sum_{j=1}^{\infty} 2^{-j} b_j \quad (2)$$

where each of the bits b_j is either a "0" or a "1", and $x \in [0,1]$. Then, the effect of the shift map applied to the binary sequence $\{b_j\}_{j=1}^{\infty}$ is described by the so-called Bernoulli shift map of Equation (3):

$$x_{k+1} = 2x_k \mod 1 \quad (3)$$

A graph representing the Bernoulli shift map is shown in FIG. 2. Referring to Equation (3), successive iterates of x are obtained by moving the separating point one position to the right (multiplication by 2) and setting to zero the first integer digit (modulo operation). Hence, digits which are initially far to the right of the separating point, and thus have only a very slight influence on the value of x eventually become the first fractional digit. In sum, a small change of the initial conditions eventually makes a large change in x_k , confirming the sensitivity to initial conditions of the chaotic Bernoulli shift.

B. Symbolic Dynamics

Symbolic dynamics may be defined as a "coarse-grained" description of the evolution of a dynamical system. The idea is to partition the state space and to associate a symbol to each partition. Then, a trajectory of the dynamical system can be analyzed as a symbolic sequence. In the case of the Bernoulli shift map, shown in FIG. 2, the state space is represented by the invariant interval $I = [0,1]$. As mentioned, the first step for characterizing the symbolic dynamics of a given dynamical system consists of introducing a proper partition of the state space. To ensure that the symbolic dynamics give rise to a topological Markov chain, a so-called Markov partition has to be selected. In the case of the Bernoulli shift map (with $N=2$), a Markov partition may be selected by simply splitting the interval $I = [0, 1]$ with respect to the critical point $c = 0.5$ and, correspondingly, we define the two subintervals $I_0 = [0, 0.5)$ and $I_1 = [0.5, 1)$, as illustrated in FIG. 2.

In order to obtain a symbolic description of the dynamics of the chaotic map under consideration, FIG. 2 associates the binary symbol "0" to the subinterval I_0 and the symbol "1" to the subinterval I_1 . Then, the evolution of the state of the Bernoulli map can be described in terms of a symbolic sequence $S = \{010010 \dots\}$.

C. Shift Register and DSP

The basic idea behind the symbolic dynamics encoder 26, which includes the shift register 16, DSP 18, and D/A converter 20 in FIG. 1, is that the Bernoulli shift process may be implemented by means of an infinite length shift register R where at each step the most significant bit (MSB) is discarded. The shift operation corresponds to a multiplication by a factor 2, while discarding the MSB at each step is equivalent to a modulo 1 operation.

A practical shift register, of course, has finite length and on the other hand it is impossible to specify the initial conditions with infinite precision. Encoding binary

data exploiting the Bernoulli shift map requires consideration of a finite-length shift register R that is fed with a binary data stream $c(k)$ to be transmitted. We assign the most recent bit of data the least significant bit (LSB) position in the shift register 16. At each step (or clock impulse) the new bit of data is copied into the LSB position of the shift register while the (old) MSB is discarded. The situation is depicted in FIG. 3(a).

We assume that the binary data stream $c(k)$ feeding the shift register is an i.i.d. (independently identically distributed) sequence. A randomization of a data stream may be obtained, if desirable, by use of a data compressor and/or a data scrambler 28, as shown in the preferred FIG. 1 embodiment, to pre-code the data stream prior to entry into the shift register 16.

1. State Quantization

In practice, due to the finite length of the shift register R , the dynamics of the Bernoulli shift can only be approximated, as the admissible states assume only discrete values. Namely, by considering a M -bit shift register, the generic state x can be expressed as:

$$x = 0.b_1b_2...b_M \equiv \sum_{j=1}^M 2^{-j}b_j \quad (4)$$

to be compared with Equation (2), where b_1 and b_M represent the MSB and the LSB, respectively. Obviously, the approximation can be made arbitrarily precise by increasing the length M of the shift register. The effect of the state quantization on the Bernoulli shift map is shown in FIG. 3(b), for the case $M = 4$.

D. Control of Chaos in the Transmitter

The preferred embodiment transmitter implements a form of predictive control with respect to the symbolic dynamics of the Bernoulli shift, with the state

definition given by Equation (4). The symbolic dynamics of the Bernoulli shift with the Markov partition are determined solely by the successive values of the MSB in the shift register R. Referring to Equation (4), the first bit on the right of the separating point determines whether the iterate falls within I_0 or I_1 (the remaining bits deciding only the relative position within I_j with $j = 0, 1$). The value of the MSB at step k coincides with the value of the LSB M steps before, at step $(k - M)$. In turn, the LSB contains the current bit of data $c(k)$. In this sense, the scheme is predictive in its nature.

The present invention solves the control problem *a priori*, by direct "synthesis" of the pseudo-chaotic signal, starting from the binary data to be transmitted. From this perspective, the injection of a new bit of data in the LSB of the shift register may be interpreted as a perturbation of the state of the dynamical system, in order to make it follow the desired symbolic sequence. The strength of the perturbation is of the order of 2^{-M} , thus can be made arbitrarily small by increasing the number M of bits of the shift register.

E. Map Shaping/Translation

The digital signal processor 18, in FIG. 1, may be realized by a Gray/binary converter. The purpose of the Gray/binary conversion is to translate the dynamics of the Bernoulli shift map, given by Equation (3), into those of the tent map, described by:

$$x_{k+1} = 1 - 2 |x_k - 0.5| \quad (5)$$

as illustrated in FIG. 4. This is done in order to achieve a greater robustness of the system in presence of noise by avoiding (zero-order) discontinuities in the map. The tent map has very similar dynamics to the Bernoulli shift map; in particular, both admit the same constant invariant density. Also, their symbolic dynamics with respect to the Markov partition can be related to each other.

1
2 In the preferred embodiment, however, the digital signal processor 18 is
3 capable of generating more complex chaotic maps. This may be useful for spectral
4 shaping purposes and/or for enhancing the Maximum-Likelihood detection.
5

6
7 F. Modulation to Produce a Transmitted Signal.

8 The signal from the digital signal processor is transformed into an analog
9 signal by the D/A converter 20, which is used to drive the modulator 22 . In the case of
10 PPM a constant offset is then added to this analog signal to form the modulation signal
11 $m(t)$ and used to drive a Pulse Position Modulator. Please note that the following two
12 sections assume the modulator 22 conducts PPM.
13

14 1. Synchronization Frame

15 In the preferred embodiment, each pulse is allocated, according to the
16 pseudo-chaotic modulation signal, within a periodic synchronization frame, as shown
17 schematically in FIG. 5. This assumes the existence of a periodic reference (with period
18 T_f) such that only one pulse train (or in the simplest case a single pulse) for each user
19 (User A or User B in FIG. 5) is transmitted within each frame time T_f , coinciding with
20 the symbol period. In FIG. 5, each frame time includes a "guard" time interval, t_g ,
21 (proportional to the constant offset) for avoiding overlapping between adjacent pulse
22 trains. Each pulse can occur at any of $N = 2^M$ (discrete) time instants, where M is the
23 number of bits of the shift register 16 and of the D/A converter 20. In FIG. 5, the timeslot
24 corresponding to each level of the pulse-position modulation has been denoted by t_s . Note
25 that the value of t_s is limited from below by the system time-base resolution.

26 Consider the case of data encoding in accordance with the symbolic
27 dynamics of the tent map. Consider the exemplary partition with respect to the critical
28 point $c = 0.5$, and indicate with t_c the corresponding time delay from the beginning of the

frame. Then, by indicating with t_k the relative time (again referred to the beginning of the frame) at which the k -th pulse train begins, if $t_k < t_c$ a "0" is being transmitted, while a "1" is being transmitted if $t_k > t_c$. The situation is shown in FIG. 5. The use of a synchronization frame enhances the robustness of coding in the presence of noise and spurious pulses by preventing error propagation phenomena.

2. Multilevel PPM

Modulation conducted in accordance with the invention may be considered a N-PPM multilevel modulation with input bit "coded" through the pseudo-chaotic map with rate $1/M$, where $M = \log_2(N)$, realizing a sort of random coded modulation. For every user bit, a number of M channel bits are transmitted and detected. N_R indicates the number of levels at the receiver. According to the invention, this may differ from the number N of levels at the transmitter. In particular, the relation $N_R \leq N$ holds, allowing a certain degree of freedom in the design of the receiver 12, and admitting classes of receivers having different complexity levels which are still capable of decoding a signal modulated in accordance with the invention.

II. Decoding

The receiver 12 decodes the signal from the channel 14. The receiver 12 includes a demodulator 30, a decoder 32 matched to the chaotic map, an output mapper 35 and a decompression/descrambling block 34.

A. Pulse Position Demodulation

In FIG. 1, the ideal detection of the incoming pulses (affected by noise) is achieved by a pulse position demodulator (PPD) 30 consisting of a pulse correlator matched to the pulse shape and a decision circuit. In the simple case of a single pulse per frame, the PPD 30 may be realized by an Integrate and Dump (I&D) filter which estimates the position of the pulse within each frame time. We assume that a normalized signal $d(t) \in [0, 1]$ is available as output of the PPD.

B. Threshold Discriminator

Demodulated data must be decoded by a decoder 32. In the simplest case the demodulator output $d(t)$ can be decoded by a simple threshold decoder. The decoder 32 is followed by an output mapper 35 and a decompressor/descrambler 34. A decision threshold 36 in the decoder 32 should be set according to the partition corresponding to $N_R = 2$, for example to the value $c = 0.5$, coinciding with the critical point of the tent map as shown in FIG. 6.

1. Coding for Noise Resistance

With the threshold detection, it is reasonable to expect that most of the error events will originate from pulses corresponding to values of the pseudo-chaotic iterates close to the partition point of the tent map ($c = 0.5$), separating the symbol "0" from the symbol "1". To reduce this particular error event probability a noise "gap" may be created in the chaotic map around its partition point c . This can be obtained by a proper pre-encoding of the data, establishing forbidden sequences of bits. One possibility is to add a code that avoids series of consecutive zeros. This constraint is usually known as run-length limit constraint and denoted by RLL $(0, k)$, where k indicates the maximum number of allowed consecutive zeros.

C. Viterbi Detection/Maximum-Likelihood Estimation

The Viterbi detector 24 performs a Maximum-Likelihood (ML) estimation of the transmitted sequence. Other techniques for deriving a sub-optimal estimator for a chaotic process in additive white Gaussian noise (AWGN) may also be used.

1. The Tent Map as a Markov Chain

Consider again the Markov partition of the invariant interval $I = [0, 1]$ of the tent map in N "states". The situation is illustrated in FIG. 6, for the case $N = 8$. From FIG. 6, transitions between different states are governed by the dynamics of the map. In

particular, only certain transitions (in this case two) are allowed from each state. For example, referring to FIG. 6, it is clear that the interval corresponding to the state 1 can only map to itself or to the state 2. More precisely, the transition taking place depends on which subinterval associated with each state, the generic iterate x_k belongs to. These two possible transitions have been labeled with 0 and 1, respectively.

Now, the Markov chain associated with the tent map (with the partition in FIG. 6) can be represented by means of an equivalent transition diagram, as illustrated in FIG. 7. The transition branches have been labeled according to the finer partition in subintervals, as discussed above and illustrated in FIG. 6. FIG. 7 also shows (within a box) the value of the output corresponding to each state, according to the encoding of the data. The trellis corresponding to the transition diagram of FIG. 7 is shown in FIG. 8

2. Detector Scalability

An interesting feature of the invention is the possibility of realizing the Viterbi detector 24 with a number N_R of states lower than the states used by a transmitter 14 to encode data. This is obtained simply by matching the Viterbi detector 24 at the receiver 12 to the map with a lower number of states. Given the transmitter number of states, N , there is a broad range of possibilities for decoding the signal produced by a transmitter implementing the invention. Receivers having Viterbi detectors with complexities $N_R = 2, 4, 8, \dots, N$, are possible. This scalability property enables receivers having different complexities and performance to decode the same transmitted signal.

3. Output Mapper/Decoding Other than Gray Conversion

When a generic chaotic map is implemented by the DSP 18 in the transmitter 10, the receiver 12 should include a further function after the detector 32 in order to exploit the scalability feature. This additional function reconstructs the

transmitted message given the estimated sequence of states provided by the detector 32 itself. This function is an output mapper, that will be, in general, a finite state machine (FSM). For particular cases and for appropriate choices of the input/output labels of the encoding map like in the Bernoulli shift and in the tent map, this FSM is not necessary.

III. Multi-user Access

Artisans will appreciate that the invention is amenable of multi-user access. For example, in the case of PPM multiple-access of the channel may be realized by assigning different pulse trains for each user and correspondingly different matched filters at the receiver side. The situation is illustrated schematically in FIG. 5, showing pulse trains associated to two different users, User A and User B. Other multiplexing techniques, like for example time-division multiplexing (TDM), may be also utilized for multiple-access purposes.

While various embodiments of the present invention have been shown and described, it should be understood that other modifications, substitutions and alternatives are apparent to one of ordinary skill in the art. Such modifications, substitutions and alternatives can be made without departing from the spirit and scope of the invention, which should be determined from the appended claims.

Various features of the invention are set forth in the appended claims.